CLAIM

1. An offline-online points system, comprising:

a main server for providing a user with an interface to submit a code, wherein the user obtained the code offline and the code is associated with N points; and

a code server for maintaining valid codes and verifying that the code that the user submitted is a valid code.

2. The system of claim 1, further comprising:

a user database that maintains an account of the user, wherein the account balance is M points prior to the user's submission of the code.

3. The system of claim 2, wherein the code server updates the account balance to M+N points after the user submits the code and if the code server verifies that the code is valid.

4. The system of claim 2, wherein the main server updates the account balance to M+N points after the user submits the code if the code server verifies that the code is valid.

5. The system of claim 2 wherein the code is C letters in length from an alphabet of L letters.

6. The system of claim 5 wherein C is 10.

7. The system of claim 6 wherein L is 29.

8. The system of claim 6 wherein L is 36.

9. A method of generating an encrypted code in base L, comprising steps:

providing an n-bit raw number;

applying a one-way hash function on the n-bit raw number with a first secret key to generate a first string;

designating an m-bit portion of the first string as an m-bit validation number; and

combining the m-bit validation number and the n-bit raw number to generate a second string.

10. The method of claim 9, further comprising steps:

applying a DES3 encryption algorithm to the second string with a second secret key to generate a third string; and

converting the third string to base L to generate the encrypted code.

11. The method of claim 9, wherein n=32, m=16, and L=29.

12. The method of claim 9, wherein the one-way hash function is MD5.

13. The method of claim 9, wherein the step of combining includes:

concatenating the m-bit validation number and the n-bit raw number.

14. The method of claim 13, wherein the m-bit validation number is the most significant bit (MSB) portion of the second string.

15. The method of claim 9, wherein the m-bit validation number is the m most significant bit (MSB) of the first string.

16. A method of verifying the validity of a code, comprising steps:

generating a code with encrypted information;

providing the code on a hard good to be distributed to users;

receiving the code online; and

verifying the validity of the code by processing the encrypted information.

17. The method of claim 16, wherein the step of generating includes steps:

providing an n-bit raw number;

applying a one-way hash function on the n-bit raw number with a first secret key to generate a first string;

designating an m-bit portion of the first string as an m-bit validation number;

combining the m-bit validation number and the n-bit raw number to generate a second string;

applying a DES3 encryption algorithm to the second string with a second secret key to generate a third string; and

converting the third string to base L to generate the code with the encrypted information.

18. The method of claim 17, wherein the step of verifying includes:

converting the code in base L to generate a first test code in base 2;

decrypting the first test code with the second secret key using a reverse DES3 encryption algorithm to generate a second test code;

applying the one-way hash algorithm to the second test code to generate a third test code; and

comparing a designated m-bit portion of the second test code to a designated m-bit portion of the third test code, and if the comparison is positive, declaring the code to be valid.

19. The method of claim 18, wherein the m-bit validation number is the m most significant bit (MSB) of the first string in the generating step and the designated m-bit portion is the most significant bit portion of the second test code and third test code in the comparing step.

20. A method for awarding incentive points to a user, comprising steps:

generating a code with encrypted information;

providing the code to an entity for printing on a hard good;

receiving the code submitted by the user; and

verifying the validity of the code by processing the encrypted information.

21. The method of claim 20, wherein the step of generating includes steps:

providing an n-bit raw number;

applying a one-way hash function on the n-bit raw number with a first secret key to generate a first string;

designating an m-bit portion of the first string as an m-bit validation number;

combining the m-bit validation number and the n-bit raw number to generate a second string;

applying a DES3 encryption algorithm to the second string with a second secret key to generate a third string; and

converting the third string to base L to generate the code with the encrypted information.

22. The method of claim 21, wherein the step of verifying includes:

converting the code in base L to generate a first test code in base 2;

decrypting the first test code with the second secret key using a reverse DES3 encryption algorithm to generate a second test code;

applying the one-way hash algorithm to the second test code to generate a third test code; and

comparing a designated m-bit portion of the second test code to a designated m-bit portion of the third test code, and if the comparison is positive, declaring the code to be valid.

23. The method of claim 22, wherein the m-bit validation number is the m most significant bit (MSB) of the first string in the generating step and the designated m-bit portion is the most significant bit portion of the second test code and third test code in the comparing step.